Lecture 11:
CryptoNET: Security Management and Protocols

Subjects / Topics:
1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

Traditional software development
• Focus on functional requirements
• Consideration of security features
  - Add-on
  - Security patches
  - Added as non-functional features
  - May introduce other bugs or vulnerabilities

Increase Complexity:
• Crypto Service Provider
• Development complexity
• Configuration complexity

Data protection standard
• Different applications different standards
• Compatibility

If IT resources are strongly protected than we can protect our environment from mobile code, malicious software, intruders, insiders' attacks and incorrect operations

Objective
Design, implement, test, and deliver high assurance information infrastructure for cryptographically protection of IT resources and operations in some data processing environment

Modules
• Security Provider
• Integrated Secure Workstation
• Software Protection
• Secure Network Communication Protocols
• Generic Secure Servers
Security standards and protocols:
- Authentication: FIPS 199, SAML Single Sign On
- Authorization & Access Control: SAML Authentication/Request & Response Protocol, XACML policies
- Secure Communication: SSL/TLS, Secure Session
- Credentials: X.509 Certificate, SAML Ticket
- Smart card: FIPS-201 (PIN)
- Encapsulation: PKCS7SignedAndEnvelopedData, S/MIME
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNet
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

---

CryptoNET: Local Authentication

- User name/password based authentication
- PIN / PIN plus fingerprint based authentication (FIPS-201)

---

CryptoNET: Strong Authentication

The identities of networked users, clients and servers are verified without transmitting passwords over the network

---

Strong Authentication: Unilateral Authentication protocols

- Entity Authentication using Public Key Cryptography
  - Unilateral Authentication
    - Single challenge-response protocol
- Mutual Authentication
  - Two challenge-response protocols
- Random number is a time variant parameter
Strong Authentication: Mutual Authentication protocols

Client

[Auth Request]

Token ID|Token BA

Token ID|Cert|Token AB

Token ID|Cert|Token BA

SA Server

Strong Authentication: Improvements

Client

[Cert A]

Token ID|Token BA

Token ID|Token AB

Token ID|Cert|Token BA

SA Server

Verify Cert A

LCA

Verify Identity

IDMS

Strong Authentication: Improvements

Client

[Cert A]

Token ID|Token BA

Token ID|Token AB

Token ID|Cert|Token BA

SA Server

Verify Cert A

App Server

Verify Cert B

IDMS

Verify Cert B

Verify Identity

Strong Authentication: Message Format

MessageBA1 = CSM(MCL/SMB RCV/alice ORG/bob TVB/e69dfb21ffd051a3 TVA/d6f47bc433299436 GSB/c26ac822a93d5c349962d1a78a229d27abfea415b934b2604e6facce2c233af5be6a9e262f5 CRB/ )

MessageBA2 = CSM(MCL/SMB RCV/alice ORG/bob TVB/e69dfb21ffd051a3 TVA/d6f47bc433299436 GSB/c26ac822a93d5c349962d1a78a229d27abfea415b934b2604e6facce2c233af5be6a9e262f5 CRB/ )

Lecture 11 :

CryptoNET: Security Management and Protocols

Subjects / Topics :

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

CryptoNET: Single Sign On

A single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords.
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

CryptoNET: Secure Session

- Secure Communication between Client and Application Server
  - Key exchange certificate
  - Session ID
  - Session Key

Secure Session
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNet
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
3. Secure Session Protocol
4. Example: Secure E-mail System

---

Example: CryptoNET: Secure Email System

Features:
- Strong Authentication
- Single Sign On
- Secure Session
- Encrypted Address Book
- Address Book Key Management
- Signed and Enveloped Email
- Efficient Handling of Attachments
- Email Confirmations
- Elimination of Spam

---

Current E-mail System

The Concept of The Extended Secure E-mail System

Extended Security Features:
- User and Server Registration
- Certificate Distribution
- Single Sign-on
- Authorization policies and Access Control
- Authorization to activate applications
- Protection of messages (confidentiality and integrity)
- Traffic protection (replay, lost messages, etc)
- Authenticity of a sender for each transaction (digital signatures)
- Authenticity of a recipient for each transaction (enveloping)
- Application Specific Security Requirements:
  - Secure multi-party transactions and protocols
  - Secure group transactions
  - Protection of user data
References

- "Entity Authentication Using Public Key Cryptography", National Institute of Standards and Technology, 1997 February 18

Questions